Published on ***ISE.gov*** (http://www.ise.gov)

ISE Business Model

The mission of the ISE is to improve the management, discovery, fusing, sharing, delivery of, and collaboration around terrorism-related information to enhance national security and help keep our people safe. Federal agencies and state, local, tribal, and private sector partners?the ISE mission partners?have the mission responsibility to help protect our people and our institutions. Consequently, these agencies deliver, and operate, the ISE and are accountable for sharing to enable end-to-end mission processes that support counterterrorism (CT).

Role of the PM?ISE

No single agency or department has the mandate or the tools necessary to empower and deliver the ISE in the same way as the PM-ISE. The role of the PM-ISE, therefore, is to coordinate and facilitate the development of a network-centric ISE by focusing on standards and architecture, security and access, associated privacy protections, and best practices. The PM-ISE serves as a change agent and enabler for innovation and discovery in providing ideas, tools, resources, and management support to mission partners who then apply them to their own agencies or communities. In particular, the PM-ISE relentlessly advocates identifying, integrating, and sharing best practices. Focus on best practices raises confidence, lowers risk, and accelerates adoption, use, and reuse of key capabilities. Examples of such reuse include:

- Reuse of standards and architecture, information exchanges, capabilities, and infrastructure;
- Reuse across the terrorism information sharing mission, across complementary missions, and into new mission areas unrelated to terrorism but important to mission partners; and
- Reuse leading to time savings and cost avoidance, bringing together the power of smart management and effective governance.

The PM-ISE uses several tools to catalyze transformation. These include:

- Information sharing and access subject matter expertise;
- Interagency policy harmonization through the White House?s Information Sharing and Access Interagency Policy Committee;
- Management and budget prioritization and follow-through via partnerships with the Office of

Management and Budget and the White House National Security Staff;

- National leadership via stakeholder engagement with mission partners and the frontline;
- Co-investment of seed capital, with mission partners, in priority early stage activities via Economy Act transactions to bridge the budgeting cycle and accelerate progress; and
- Ability to bring together mission partners to identify and address common mission equities.

The importance of these tools and mandates becomes clear in filling the gaps in budgetary considerations which challenge the ability of any single organization to achieve the goals of sharing information. Seeding new initiatives or transformation of existing capabilities is hard; and even more so in government where funding constraints and long-lead times make budgeting for new initiatives difficult. Addressing inherent interdependencies is at the core of the office?s ability to respond to and support its partners.

The PM-ISE?s aim is always to develop these initiatives in full partnership with mission owners. In addition, as improved business processes, supporting policies, and technical solutions are developed and deployed, the PM-ISE helps identify, promote, and spread best practices and, where possible, influences resource allocation decisions to ensure the institutionalization and potential reuse of these mission partner capabilities.

In carrying out the responsibilities of the office, the PM-ISE employs three engagement models:

- For a small number of core priorities?such as SAR, SBU Networks, and fusion centers?the Program Manager engages directly to help drive progress. The goal with these efforts is transactional: to first drive transformation in conjunction with mission partners, to then help the mission partners in planning for broader implementation of the transformed effort, and ultimately to decrease involvement.
- The PM-ISE supports a consistent set of enablers, such as privacy, information assurance, and standards and architecture. This support is ongoing, not transactional, although engagement will spike around specific challenges or opportunities.
- Finally, the PM-ISE is committed to broadly sourcing, integrating, and sharing best practices. The PM is recognized as a champion for information sharing by agencies at all levels of government, and receives and supports requests for reuse and ramp-up of sharing best practices.

A major strength of the ISE business model has been its flexibility, a necessity for operating in uncharted waters. The expanding influence of the ISE is the result of continued success in serving our mission partner partners, the organizations ultimately responsible for the delivery and operation of the ISE.

Central Role of Mission Partners

The ISE is realized by the investment of mission partners and made relevant through use by frontline law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel. Ultimately, the ISE is neither more nor less than the contributions of the ISE mission partners, augmented by core capabilities and ISE enablers. Over the last several years, information sharing centers of excellence have emerged across government. These centers have developed independently and adopted different approaches to sharing information across all levels of government, but they share a common commitment to using the power of information to help keep our people safe.

Terrorism?Related Information and Beyond

The focus of the ISE is specifically on the sharing of terrorism and homeland security information. The

need for collaboration and sharing of information, however, extends beyond terrorism-related issues to encompass all information relevant to the national security of the United States and the safety of the American people. Information does not typically come neatly packaged and labeled to indicate its subject matter or domain of interest. Information from one domain may prove valuable in another, often at a different time and in another form. Information that initially surfaces in the public health domain may later be determined to have implications for counterterrorism, and vice versa. Given that, the ISE must reach out to other information sharing activities at all levels of government to ensure effective information sharing and access, while protecting privacy and information security, across all domains that may potentially process or handle terrorism-related information.

Consequently, ISE mission partners rarely have the ability to segregate their activities to isolate terrorism information. Frontline law enforcement, for instance, is more likely to generate SARs relating to gang or narcotic crime than criminal activity with a clear terrorism nexus. The inherent adaptability of the business process developed as part of the Nationwide SAR Initiative (NSI) allows mission partners to capitalize on consistent training, privacy and civil liberty protections, oversight, and change management investments developed for the ISE and apply these capabilities more broadly to allcrimes, all-hazards operations. Such mission partner needs must be factored into ISE strategy and plans to avoid deadlock and inefficient or ineffective solutions.

Major ISE Initiative Transitions

Four ISE initiatives have transitioned from PM-ISE sponsorship to agency management over the last four years.

A May 2008 Presidential Memorandum designated National Archives and Records Administration (NARA) as the Executive Agent responsible for creating and carrying out a government-wide framework for CUI, effectively transitioning responsibility for this effort from PM-ISE to NARA.

Although many agencies were involved with the establishment of the Interagency Threat Assessment and Coordination Group (ITACG), the PM-ISE was a strong proponent and worked closely with other agencies to see that the ITACG was properly funded and staffed. (The PM-ISE continues to report on its progress to the Congress each year.) Subsequently, the host agency, the National Counterterrorism Center (NCTC) and lead analytic agencies (the Department of Homeland Security (DHS) and the FBI) assumed full responsibility for ITACG management in February 2008.

Since the last ISE Annual Report, two major programs graduated from the concept stage and are taking steps towards full nationwide implementation. On December 17, 2009, the President?s Assistant for Homeland Security and Counterterrorism reported that Homeland Security Secretary Napolitano agreed to establish a multiagency program management office (PMO) ?to coordinate support for a growing network of state and major urban area fusion centers,? and that Attorney General Holder agreed to establish a multiagency PMO (in the Justice Department?s Bureau of Justice Assistance (BJA)) ?charged with developing a nationwide framework for reporting suspicious activities.?

The memorandum went on to say:

> Establishing dual PMOs will institutionalize two essential national security initiatives. The fusion center concept and an overall suspicious activity reporting approach have matured under the auspices of the Program Manager, Information Sharing Environment, and through the hard work of collaborating departments and agencies and other contributors ? Going

forward, leadership by the Departments of Homeland Security and Justice will provide dedicated attention to speed effective implementation.

These transitions validate the assumptions underlying the overall ISE business model. As additional ISE efforts mature sufficiently, they will follow a similar path: starting out with strong PM-ISE sponsorship and support and, ultimately, assigning lead responsibility to the mission partner best postured and equipped to fully institutionalize the capability.
